Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Monday 25 April 2022 - Monday 16 May 2022

Supervised hours 4 hours

Paper reference **20158K**

Information Technology

UNIT 11: Cyber Security and Incident Management

Part B

You must have:
Forensic_Analysis.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- Learners **must only** have access to **Part B** during this supervised assessment period.
- This booklet should be kept securely until the start of the 4-hour, **Part B** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- **Part A** must not be accessed during completion of **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** task must be submitted together for each learner.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this Part is 37.

Turn over ▶

R71612A

1/1/1/1/1/1/

Pearson

Instructions to Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of 3 weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 4-hour **Part B** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

An electronic template for activity 4 is available on the website for centres to download for learner use.

Learners must complete **Part B** on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in **Part B** but cannot provide any guidance in completion of the task.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is **not** permitted.
- Learners' work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely, and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part B**, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work.

The folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

Each learner will need to submit 2 PDF documents within their folder.

The 2 PDF documents should use these file names:

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 18 May 2022.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is **not** allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in this task but cannot provide any guidance in completion of the activities.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work.

The folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

You will need to submit 2 PDF documents within this folder.

The 2 PDF documents should use these file names:

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work in to your invigilator.

Set Task Brief

The Gangala Aventurparko

The Gangala Aventurparko is in the country of Varma Loko and is one of several tourist attractions owned by Varma Loko Leisure Parks (VLLP).

Gangala Aventurparko has recently had a new IT system installed. The system is being used as a pilot project for improvements at all VLLP sites. The Project Manager is Viro De Ordoni.

Figure 1 shows a map of the park and the area around it.

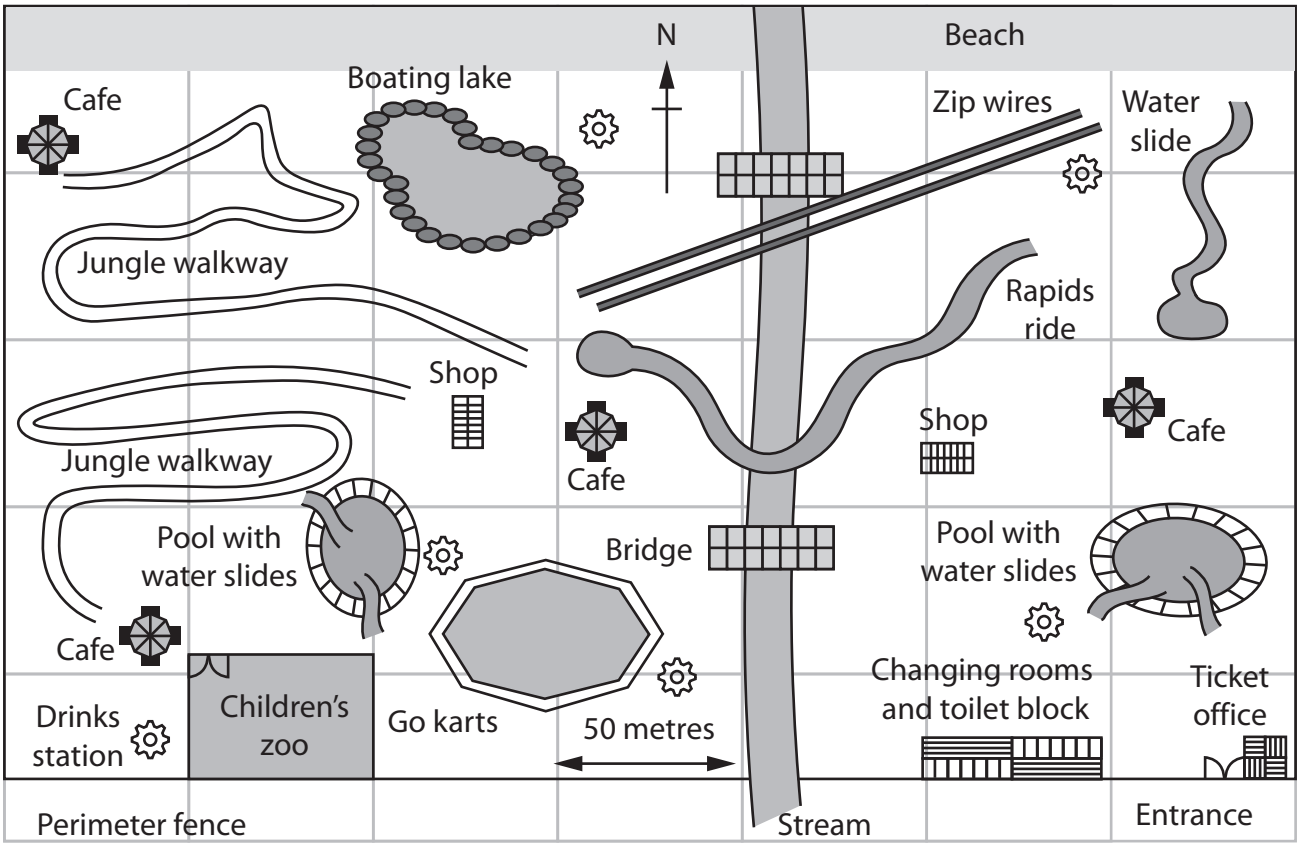


Figure 1

On entering the park, each visitor is given a wristband containing an RFID chip linked to a personal VLLP account. The account can be preloaded with credit at the ticket office or at one of the shops.

When visitors use one of the paid attractions or buy something at a shop, cafe or drinks station, their RFID chip is read. Then payment is taken from the visitor's VLLP account.

Visitors may also link their account to a credit card so that they do not need to preload. Payment is then taken from their credit card when the visitors leave the park.

The point of sale equipment in the ticket office, shops and cafes accepts cash or cards.

The point of sale equipment at attractions or drinks stations only uses the RFID system for payment.

Client brief

You advised VLLP on cyber security matters when Gangala Aventurparko was being planned. Now, a few months later, Viro has asked you to review the investigation of a cyber security incident.

The incident occurred in late April.

Guests reported that their accounts were being charged for items that they had not purchased. A member of the sales staff checked the records and alerted the duty technician.

The duty technician realised that there was a potential system breach and contacted VLLP Head Office.

Evidence items from the security incident at Gangala Aventurparko

Evidence items include:

1. Team Leader's report
2. Drinks station operations report
3. Drinks station logs
4. Network diagram
5. Cyber security document – incident management policy.

1) Team Leader's report

Incident Number 220304

Mon. 25th April. 2022. 13:00

Zorge Boffinon: Manager, VLLP technical support team

Situation

A system intrusion at Gangala Aventurparko was reported to VLLP Head Office at 15:26 on Saturday 23rd April. The duty technician at Gangala Aventurparko, Konto Frostujo, said that a customer account had been compromised. He had frozen the account as a precaution.

I logged the report as being a cyber-security incident. Then I co-opted Mr. Rilato of the Public Relations department to assist.

I contacted the Legal department, but they only had a few staff at the weekend. They said that Mr Rilato should make the first on-site assessment and legal staff could be called in if the incident was considered serious enough.

Mr. Rilato and I met with Mr. Frostujo at the park ticket office at 15:55.

Mr. Frostujo reported that he had been alerted to a problem by ticket office staff at 15:10 on 23rd April. Visitors leaving the park are given itemised receipts when they pay their bills. One family had complained about items that they did not believe they had purchased.

This is not an unusual event as people do forget things, or try to avoid payment. There are CCTV cameras at shops, cafes and attractions around the park, so it is usually simple to see if the purchase has been made at the time and place shown.

The ticket office staff had passed the family on to Mr. Frostujo who checked the video recordings. It was clear that they had not made the logged purchases and Mr. Frostujo had followed the normal procedure of freezing the account and contacting VLLP Head Office.

On-site investigation

The team met with the family and Mr. Rilato assured them that all charges on their account would be removed.

The team then reviewed the purchase logs **(see evidence item 3)** and video evidence. It was noted that:

- two false purchases were made
- the false purchases were at a drinks station
- the family were not at the drinks station at the time of purchase
- the family could be seen nearby in the video footage.

Drinks station operations are explained in a separate report **(see evidence item 2).**

Second event

16:43 on Saturday 23rd April.

Shortly after the log and video review, another visitor complained about an incorrect bill for two drinks. On investigation it was obvious that the circumstances were the same, except for a different drinks station being used **(see evidence item 3)**. The visitor's bill was cancelled, and the event was added to the current incident.

Conclusions

The team concluded that there were three possible causes.

1. A bug in the drinks station or billing software.
2. An error in setting up the wristband chips for the customers involved.
3. An attack on the RFID identification/authorisation system.

Remedial action

It is possible that there is a bug but the team concluded that it was impossible to prove as the software and hardware is proprietary and supplied by an outside company.

Wristband setup was reviewed. A dummy purchase was added to the procedure to check that each chip is connected to the correct account.

The use of a PIN in making an RFID purchase was discussed and the decision was deferred pending a management meeting at VLLP Head Office.

Addendum Thursday 28th April

VLLP senior managers conferred with the Legal and Public Relations departments and decided that it was not in the company's commercial interest to implement a PIN on RFID purchases. The use of a PIN will not be introduced.

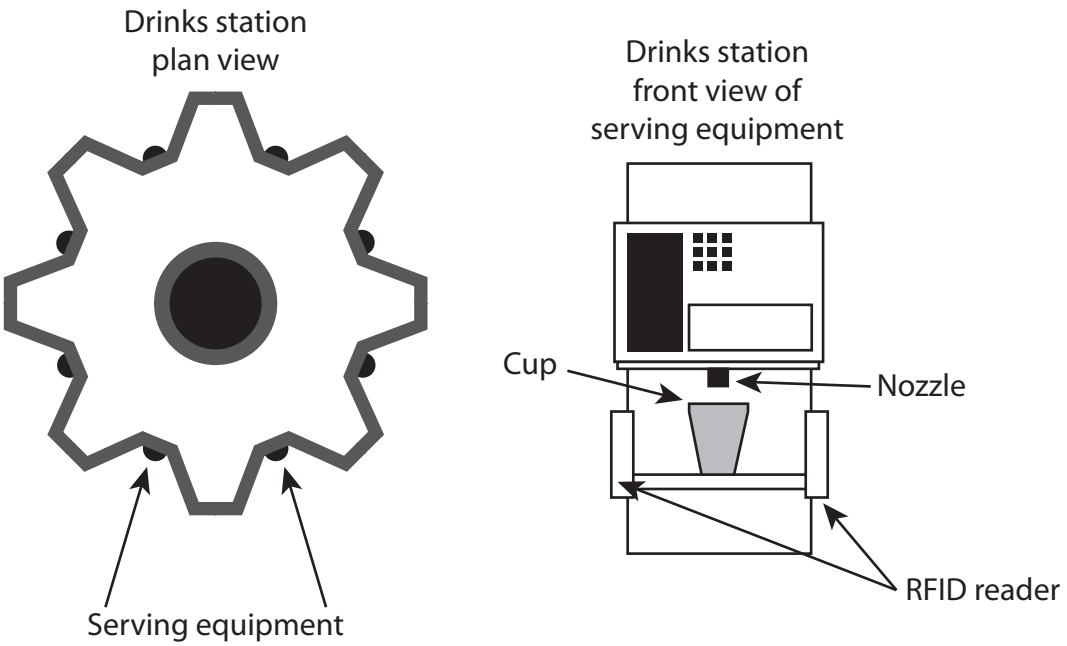
BLANK PAGE

2) Drinks station operations report

Text of operating instructions displayed at each set of serving equipment.

Drinks dispenser

1. Choose your drink by pressing the correct button on the display panel.
2. Hold your cup in the hand with your payment wristband.
3. Place the cup under the dispensing nozzle.
4. The chosen drink will be served automatically.
5. Remove the cup when the flow of drink stops.



Operating notes

The RFID readers have a read-range of 30cm.

The nozzle has an active IR system that detects the presence of a cup.

Drink dispensing starts on:

- drink selected

  and

- cup present

  and

- wristband present with enough credit or link to a payment card.

Drink dispensing ends on:

- cup removal

  or

- wristband out of range

  or

- pre-set volume served.

Drinks station security

The stations are fully automatic and only accept RFID payment. Malfunction reports are sent to the Maintenance department via the network.

Each station is within the view of a CCTV camera. The cameras are designed and sited to cover larger areas of the park, not just the drinks stations.

3) Drinks station logs

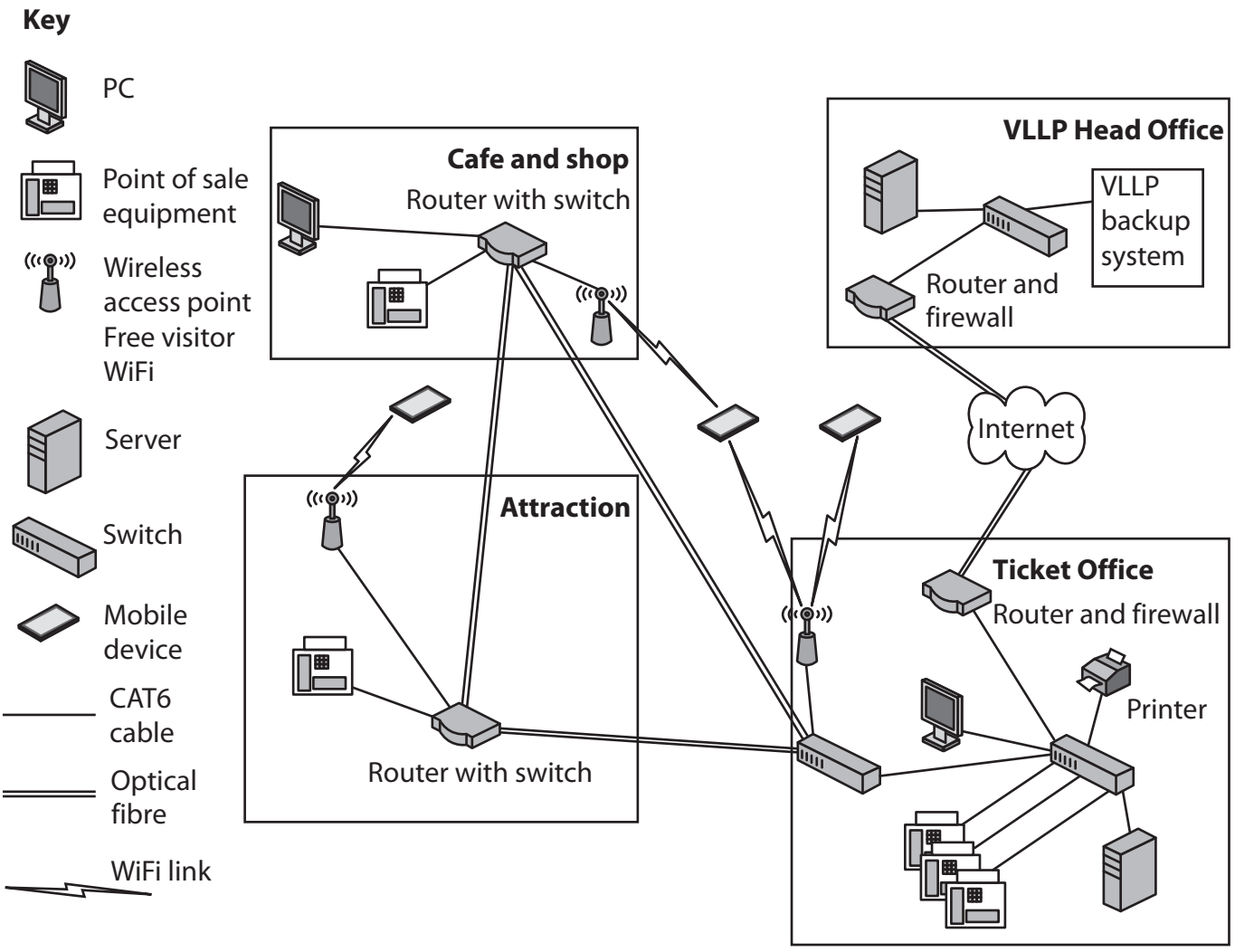
Extract from log for drinks station B (First event)
Payment card numbers redacted, last four figures only are shown.

Time stamp	Nozzle	Chip ID	Drink	Payment card	Notes
23041232	3	1153	6	xxxx-xxxx-xxxx-2327	
23041232	7	2285	5		
23041232	5	2412	2	xxxx-xxxx-xxxx-7666	
23041233	4	3127	2		
23041233	2	2338	7	xxxx-xxxx-xxxx-5354	
23041233	8	1187	7	xxxx-xxxx-xxxx-4476	
23041233	6	2935	9	xxxx-xxxx-xxxx-7759	Cherry slush, disputed
23041233	7	2285	5		
23041234	6	2935	1	xxxx-xxxx-xxxx-7759	Apple slush, disputed
23041234	3	3362	6	xxxx-xxxx-xxxx-3221	
23041234	8	1822	6	xxxx-xxxx-xxxx-9709	
23041234	4	3127	2		
23041234	1	2887	9	xxxx-xxxx-xxxx-2444	
23041234	5	2412	2	xxxx-xxxx-xxxx-7666	
23041235	1	2887	9	xxxx-xxxx-xxxx-2444	
23041235	2	1003	4	xxxx-xxxx-xxxx-6561	
23041235	6	1709	3	xxxx-xxxx-xxxx-4423	
23041235	8	1232	7	xxxx-xxxx-xxxx-3390	
23041235	2	1003	4	xxxx-xxxx-xxxx-6561	
23041235	4	3127	1		

Extract from log for drinks station D (Second event)
Payment card numbers redacted, last four figures only are shown.

Time stamp	Nozzle	Chip ID	Drink	Payment card	Notes
23041602	1	1153	6	xxxx-xxxx-xxxx-2327	
23041602	6	2285	5		
23041602	2	3362	2	xxxx-xxxx-xxxx-3221	
23041602	4	3127	2		
23041603	6	2338	7	xxxx-xxxx-xxxx-5354	
23041603	3	1187	7	xxxx-xxxx-xxxx-4476	
23041603	8	2412	9	xxxx-xxxx-xxxx-7666	Cherry slush, disputed
23041603	2	2285	5		
23041603	1	2887	1	xxxx-xxxx-xxxx-2444	
23041604	2	3362	6	xxxx-xxxx-xxxx-3221	
23041604	8	1822	6	xxxx-xxxx-xxxx-9709	
23041604	5	3127	2		
23041604	1	2887	9	xxxx-xxxx-xxxx-2444	
23041604	8	2412	1	xxxx-xxxx-xxxx-7666	Apple slush, disputed
23041604	3	1755	9	xxxx-xxxx-xxxx-6647	
23041605	7	1003	4	xxxx-xxxx-xxxx-6561	
23041605	4	1709	3	xxxx-xxxx-xxxx-4423	
23041605	1	2887	7	xxxx-xxxx-xxxx-2444	
23041605	8	1033	4	xxxx-xxxx-xxxx-6665	
23041605	5	3127	1		

4) Network diagram



BLANK PAGE

Turn over ▶

5) Cyber security document – incident management policy

Incident management team

The Computer Security Incident Response Team (CSIRT) shall consist of:

- a Technical Manager from VLLP Head Office (Team Leader)
- the senior technician present at the affected site at the time of the incident.

If the Team Leader suspects that customer data may have been compromised, the VLLP Legal and Public Relations teams shall be informed and representatives appointed.

The Team Leader shall co-opt other team members as needed.

Incident reporting

Any member of staff who considers that an IT-related security incident has occurred must report it as soon as possible to the Team Leader.

Initially it may be reported verbally but this must be followed up by an email. It is the responsibility of the CSIRT to maintain detailed documentation on the incident from first report to final resolution.

Security incidents may include:

- theft of IT equipment
- theft of company data
- unauthorised access to VLLP systems
- infection of VLLP systems with malware.

Incident response procedures

(a) **Theft of IT equipment**

- Theft of IT equipment is a very serious issue. Any thefts must be reported at once to the CSIRT leader, initially a verbal report must be made followed up by email, providing as much information as possible (location and type of equipment, when it was last seen etc.).
- The CSIRT leader must ascertain if the item has actually been stolen (or if it is just missing).
- If the item is confirmed as stolen, the CSIRT leader must inform the VLLP Finance department so they can inform insurers.
- The CSIRT must prepare a report on the theft for VLLP, and if needed justify the finances required to replace the stolen item.

(b) **Theft of data**

- Theft or loss of data may occur in a number of different ways.
- Any loss of data must be reported at once to the CSIRT leader, initially a verbal report must be made followed up by email.
- The CSIRT must investigate the loss and identify exactly what data has been lost or stolen and when the incident occurred.
- Where it is suspected that customers' personally identifiable information has been accessed a report must be made to the VLLP Legal and Public Relations teams.
- Having identified what has been lost or stolen and when, the CSIRT must retrieve backups and restore the data as soon as possible.
- The CSIRT should review the incident and implement procedures to prevent future losses.

(c) Infection of IT systems with malware

- Any member of staff who suspects that any IT system has been infected with malware must report at once to the CSIRT leader, initially a verbal report must be made followed up by email.
- The infected system should be shut down as soon as possible.
- The CSIRT will investigate the infection and take appropriate measures to resolve the infection and restore the system.

(d) Unauthorised access to systems

- Any member of staff who suspects that there has been unauthorised access to any system must report it at once to the CSIRT leader, providing as much detail as possible (which system, how access was obtained). Initially a verbal report must be made, followed up by email.
- The CSIRT will thoroughly investigate the incident and identify how the unauthorised access was obtained.
- The CSIRT will take whatever action is required to prevent future occurrences (e.g. change passwords).

Part B Set Task

You must complete ALL activities within the set task.

Produce your documents using a computer.

Save your documents in your folder ready for submission using the formats and naming conventions indicated.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You have been advising Viro De Ordoni on cyber security. Now he has asked you to review the investigation of a cyber security incident.

Activity 4: Forensic incident analysis

Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident at Gangala Aventurparko.

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1–4 inclusive.

Produce a forensic incident analysis using the template **Forensic_Analysis.rtf**

Save your completed forensic incident analysis as a PDF in your folder for submission as **activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 4 = 14 marks)

Activity 5: Security report

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future.

Areas for improvement are:

- adherence to forensic procedures
- the forensic procedure and current security protection measures
- the security documentation.

Read the set task brief and evidence items 1–5 inclusive when answering the question.

Save your completed security report as a PDF in your folder for submission as **activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 5 = 20 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART B = 3 MARKS

TOTAL FOR PART B = 37 MARKS